UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/067,319	02/07/2002	Swati Deshmukh	01.261.01 (920-0150US)	7037

13205 7590 08/15/2011

McAfee-Wong Cabello Lutsch Rutherford & Brucculeri
LLP
20333 Tomball Parkway, 6th Floor
Houston, TX 77070

EXAMINER	
NGUYEN, QUANG N	
ART UNIT	PAPER NUMBER
2441	
NOTIFICATION DATE	DELIVERY MODE
08/15/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

wcpatent@counselip.com
cmiles@counselip.com
sconroy@counselip.com

UNITED STATES PATENT AND TRADEMARK OFFICE

____

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

____

Ex parte SWATI DESHMUKH, SUNIT KADAM, and MIKE BACUS

____

Appeal 2009-011169
Application 10/067,319
Technology Center 2400

____

Before ERIC S. FRAHM, JASON V. MORGAN, and ERIC B. CHEN, *Administrative Patent Judges*.

FRAHM, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Introduction

Appellants appeal under 35 U.S.C. § 134(a) from a final rejection of claims 1, 16, 17, 32, 33, and 48-81. Claims 2-15, 18-31, and 34-47 have been canceled. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

Exemplary Claim

Exemplary independent claim 1 under appeal, with emphasis added, reads as follows:

> 1. A method of reporting malware events comprising the steps of:
>
> detecting a plurality of malware events each with one of a plurality of levels using a malware scanner, the plurality of malware events comprising completion of a malware scan, a process failure relating to malware scanning, a missing log file, detection of malware, and failure of a response to malware;
>
> determining a level of a detected malware event;
>
> comparing the level of the detected malware event to an event trigger threshold with one of a plurality of levels; and
>
> transmitting a notification of the detected malware event over a network, based on the comparison of the level of the detected malware event to the event trigger threshold;
>
> wherein the level of the detected malware event comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the level of the event trigger threshold comprises one of: informational malware events requiring no operator intervention; warning malware events that indicate a process failure; minor malware events that require attention, but are not events that could lead to loss of data; major malware events that need operator attention; critical malware events that need immediate operator attention and could lead to loss of data if not corrected;

wherein the transmitting step comprises the steps of: transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and *transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold*;

wherein the event trigger threshold is configurable to control an amount of the notifications that are received in real-time so as to prevent network congestion that adversely affects the usability of the network.

The Examiner's Rejections

The Examiner rejected claims 1, 16, 17, 32, 33, and 48-81 as being unpatentable under 35 U.S.C. § 103(a) over the combination of Ackroyd (US 2003/0131256 A1) and Hansen (US 6,493,755 B1). Claims 1, 17, and 33 are the only independent claims, and each recite: "transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold" (claims 1, 17, and 33).

The Examiner's Findings

In making the rejection listed above, the Examiner relies upon Ackroyd as teaching or suggesting all of the claimed subject matter except for (i) transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold; and (ii) transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold (Ans. 4-7). The Examiner relies upon Hansen to cure these two deficiencies cited in Ackroyd. The Examiner determines that the two features missing from Ackroyd would have been obvious to the ordinarily skilled artisan in view of the teachings and suggestions of Hansen, namely column 4, lines 20-35 of Hansen (Ans. 8 and 11-12).

Appellants' Contentions

Appellants contend that the Examiner erred in rejecting claims 1, 16, 17, 32, 33, and 48-81 under 35 U.S.C. § 103(a) over the combination of Ackroyd and Hansen for numerous reasons, including that Hansen fails to teach or suggest "transmitting the notification of the detected event eventually, if the level of the detected malware event is less than the event trigger threshold," as recited in claims 1, 17, and 33 (Reply Br. 4-6).

Issue on Appeal

Did the Examiner err in rejecting claims 1, 16, 17, 32, 33, and 48-81 as being obvious because the combination of Ackroyd and Hansen fails to teach or suggest the limitation of "transmitting the notification of the detected event eventually, if the level of the detected malware event is less than the event trigger threshold," as recited in independent claims 1, 17, and 33?

ANALYSIS

We agree with Appellants' contention specifically addressed *supra*.

The combination of Ackroyd and Hansen teaches transmitting the notification of the detected malware event in real-time, if the level of the detected malware event is greater than or equal to the event trigger threshold (Ans. 8 (citing Hansen, col. 1, ll. 40-43, col. 1, ll. 57 to col. 2, l. 44, and col. 4, ll. 20-35)). However, Hansen fails to teach or suggest transmitting the notification of the detected malware event eventually, if the level of the detected malware event is less than the event trigger threshold, as set forth in claims 1, 17, and 33 (*see* Hansen, col. 4, ll. 20-35, disclosing that a notification of event status is made only when preselected and defined network events occur, not when a level of detected malware event is less than the detected threshold as claimed). The Examiner has not provided adequate reasoning or explanation as to how Hansen's column 4, lines 20-35 constitutes or suggests the timing (i.e., eventually instead of in real-time) of notification "if the level of the detected malware event is less than the event trigger threshold," as set forth in claims 1, 17, and 33 (*see* Ans. 8 and 11-12). Moreover, the Examiner's use of Hansen's teachings of choosing different notification actions, such as executing a script, making a sound, or writing to an event log are inadequate (*see* Ans. 7; *see also* Hansen, col. 2, ll. 31-43). The claimed invention invokes only one form of "transmitting a notification," with the timing of the notification based on the level of the detected malware event and an event trigger threshold. The Examiner has not shown that any one of Hansen's notification actions, such as executing a script, would eventually take place as a result of taking a different action, such as writing to an event log.

CONCLUSIONS

(1) Hansen fails to teach or suggest the limitation of "notification of the detected event eventually, if the level of the detected malware event is less than the event trigger threshold," as recited in claims 1, 17, and 33.

(2) Appellants have established that the Examiner erred in rejecting claims 1, 16, 17, 32, 33, and 48-81 as being unpatentable under 35 U.S.C. § 103(a).

(3) Claims 1, 16, 17, 32, 33, and 48-81 have not been shown to be unpatentable.

DECISION

The Examiner's rejections of claims 1, 16, 17, 32, 33, and 48-81 are reversed.

REVERSED

msc